STEVENS & SHOWALTER, L.L.P.

Attorneys at Law

RICHARD C. STEVENS
ROBERT L. SHOWALTER*
THOMAS E. LEES

OF COUNSEL

MICHAEL D. FOLKERTS
CHARLENE L. H. STUKENBORG

* ALSO ADMITTED IN KENTUCKY

7019 CORPORATE WAY
DAYTON, OHIO 45459-4238

PATENTS, TRADEMARKS,
COPYRIGHTS & RELATED MATTERS

TELEPHONE (937) 438-6848
FACSIMILE (937) 438-2124
EMAIL: SSLLP@SPEAKEASY.NET

FACSIMILE TRANSMISSION

TO:	Name:	Examiner Matthew T. Henning, Art Unit 2131	
	Company:	US Patent and Trademark Office	
	Fax No.:	571-273-8300	Phone No.:

FROM:	Name:	Thomas E. Lees, Reg. No. 46,867	
	Date:	November 17, 2006	
	Our. Ref.:	Serial No.09/921,536; Docket 5577-236 (RSW920000185US1-IBM019PA)	Trans. No.:

# Pages (incl. cover):	9

REMARKS:

OFFICIAL

NOTICE OF APPEAL (2 copies for charge to deposit account) and PRE-APPEAL BRIEF REQUEST FOR REVIEW

Please deliver to Examiner Henning

RECEIVED
CENTRAL FAX CENTER
NOV 17 2006

Doc Code: AP.PRE.REQ

PTO/SB/33 (07-05)
Approved for use through xx/xx/200x. OMB 0651-00xx
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PRE-APPEAL BRIEF REQUEST FOR REVIEW

Docket Number (Optional): 5577-236 (IBM 019 PA)

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to "Mail Stop AF, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450" [37 CFR 1.8(a)] or facsimile submitted to 571-273-8300. on Nov. 17, 2006

Signature: Thomas E. Lees

Typed or printed name: Thomas E. Lees

Application Number	Filed
09/921,536	08/03/2001

First Named Inventor: John McGarvey

Art Unit	Examiner
2131	Matthew T. Henning

Applicant requests review of the final rejection in the above-identified application. No amendments are being filed with this request.

This request is being filed with a notice of appeal.

The review is requested for the reason(s) stated on the attached sheet(s).
Note: No more than five (5) pages may be provided.

I am the

- ☐ applicant/inventor.
- ☐ assignee of record of the entire interest. See 37 CFR 3.71. Statement under 37 CFR 3.73(b) is enclosed. (Form PTO/SB/96)
- ☐ attorney or agent of record. Registration number _____
- ☑ attorney or agent acting under 37 CFR 1.34. Registration number if acting under 37 CFR 1.34: 46,867

Signature: Thomas E. Lees

Typed or printed name: Thomas E. Lees

Telephone number: 937/438-6848

Date: Nov. 17, 2006

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below*.

☐ *Total of _____ forms are submitted.

Attorney Docket 5577-236 (RSW920000185US1-IBM 019 PA)
Serial No. 09/921,536

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant	: McGarvey et al.
Serial No.	: 09/921,536
Filed	: August 03, 2001
Title	: Methods, Systems and Computer Program Products For Secure Delegation Using Public Key Authorization
Attorney Docket	: 5577-236 (RSW920000185US1-IBM 019 PA)
Examiner	: M. Henning
Art Unit	: 2131
Confirm	: 6803

CERTIFICATE OF FACSIMILE TRANSMISSION

I hereby certify that this correspondence is being facsimile transmitted to the Patent and Trademark Office at fax no. ((571)273-8300) on November 17, 2006.

Thomas E. Lees — 46,867 Reg. No.

Mail Stop AF
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

ARGUMENTS IN SUPPORT OF APPLICANTS' PRE-APPEAL BRIEF REQUEST FOR REVIEW

This paper is submitted with the applicants' Notice of Appeal and Pre-Appeal Brief Request for Review in response to the Office action made Final dated August 18, 2006.

Status of the Application

Claims 1-32 are pending. Claims 1, 23-29 and 31-32 stand rejected under 35 U.S.C. §103(a) as being obvious over U.S. Pat. App. Pub. No. 2003/0018913 to Brezak et al. (hereinafter 'Brezak') in view of U.S. Pat. No. 5,535,276 to Ganesan (hereinafter 'Ganesan'). Additionally, claims 2, 3, 5, 7-11, 14, 15 and 30 stand rejected under 35 U.S.C. §103 a being unpatentable over Brezak in view of Ganesan and further in view of U.S. Pat. No. 6,829,356 to Ford (hereinafter 'Ford'). Still further, claims 4, 6, 12, 13 and 20 stand rejected under 35 U.S.C. §103 a being unpatentable over Brezak in view of the Ganesan, Ford and further in view of "Applied Cryptography" by Schneier (hereinafter 'Schneier'). Still further, claims 16-19 and 21-22 stand rejected under 35 U.S.C. §103 a being unpatentable over Brezak in view of Ganesan, Ford and further in view of "Handbook of Applied Cryptography" by Menezes et al. (hereinafter 'Menezes').

The Art of record Fails to Establish a *Prima Facie* Case of Obviousness

The applicants assert that the art of record fails to establish a *prima facie* case of obviousness because the prior art references, even when combined, fail to teach or suggest all the claim limitations[1]. For example, Claim 1 recites in pertinent part:

> obtaining a common nonce associated with each of the plurality of servers from an entity other than the client or the plurality of servers;
> providing the common nonce to the client;
> receiving the common nonce signed by the client at the middle-tier server; and
> providing the signed common nonce to the plurality of servers as a signature for transactions so as to authenticate the client to the plurality of servers.

The Office Action asserts that Brezak discloses all of the recitations of Claim 1 with the exception of "...receiving the common nonce signed by the client at the middle-tier server", which the Office Action asserts is disclosed by Ganesan[2]. In support of this position, the Examiner attempts to read the claimed "...common nonce associated with each of the plurality of servers from an entity other than the client or the plurality of servers" onto the "privilege attribute certificate" (PAC) disclosed by Brezak[3]. Contrary to the Examiner's conclusion, it is the applicants' position that, when reading claim 1 *as a whole*, Brezak *can not* teach or suggest this claim element.

A "privilege attribute certificate" (PAC) 404 as taught by Brezak[4], includes delegation information such as a "component identity information" field and an "access restriction information" field. The component identity information field stores a history of servers that request a *service ticket* on behalf of the client. The access restriction information selectively identifies certain servers/services that client has either directly, or indirectly designated as allowing the first server to delegate to[5]. Thus, the PAC is a set of data fields maintained by a trusted third party for tracking the history and access restrictions of requests for service tickets on behalf of a client and is not a *common nonce associated with each of the plurality of servers*.

---

[1] See for Example, the M.P.E.P. §706.02(j).
[2] See Office Action mailed 08/18/2006, starting at Page 3, line 17 to Page 4, line 5.
[3] See Office Action mailed 08/18/2006, Pages 2-3.
[4] See Fig. 4 of Brezak

Even assuming *arguendo*, that the PAC can be treated as a common nonce associated with each of the plurality of servers, (which the applicants strongly urge it cannot), Brezak still fails to teach or suggest that the PAC, which is provided to the client is also provided to the plurality of servers as a signature for transactions so as to authenticate the client to the plurality of servers, as claimed. In Brezak, several layers of transactions separate the PAC received by the client from the PAC communicated to the back-end servers. In order to see this, it is important to understand the transaction method utilizes by Brezak.

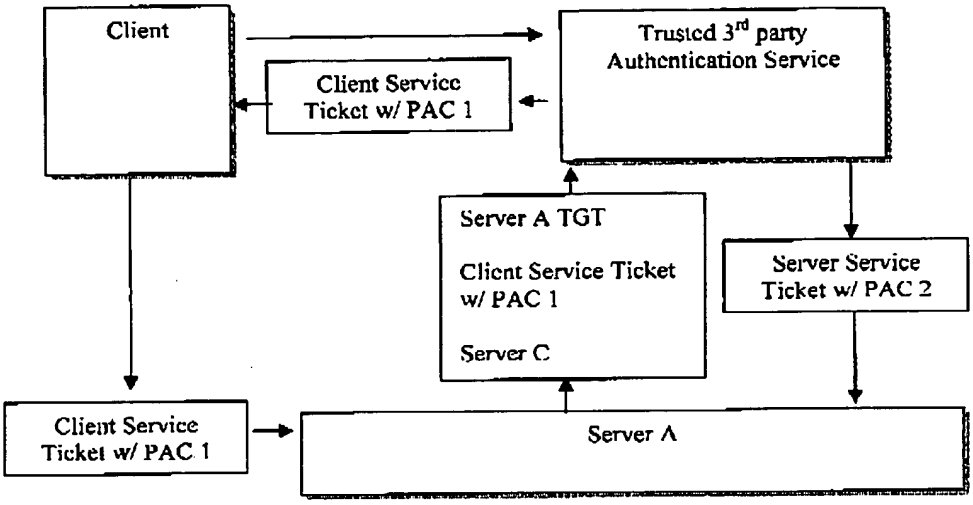
As disclosed in Brezak, in order for a client 202 to access Server A, the client 202 and Server A each first obtain a "Ticket Granting Ticket" (TGT) from a trusted third party authentication service 206[6]. The client then sends a ticket granting service request message to the authentication service 206. The authentication service replies to the client 202 with a message 226 that includes a *client service ticket*, which is associated with both the client 202 and Server A. This ticket may include a first PAC as described above. Before initiating a communication session, the client sends this *service ticket* to Server A[7]. In the disclosed example in Brezak, it is assumed that Server A needs to access Server C on behalf of the client 202[8]. Thus, Server A sends its *own* ticket granting service request message to the third party authentication service 206. The request by Server A includes Server A's previously obtained Ticket Granting Ticket, the *client's service ticket* (which may include a first PAC) and the identity of the target server (Server C in this example)[9].

The authentication service 206 checks to see if the client 202 has authorized delegation in response to receiving the ticket granting service message from Server A. If the authentication service 206 determines that it is okay to delegate, it replies to Server A with a reply message that includes a *new* service ticket for Server A. The reply message *may also* provide client account data in the form of a second PAC. There are two possible sources of the PAC information in *Server A's* service ticket. The PAC may be derived by the third party authentication service, e.g., from an

---

[5] See Brezak, U.S. Pat. Pub. No. 2003/0018913, paragraphs 50-52.
[6] See Brezak, U.S. Pat. Pub. No. 2003/0018913, paragraph 42.
[7] See Brezak, U.S. Pat. Pub. No. 2003/0018913, paragraph 43.
[8] See Brezak, U.S. Pat. Pub. No. 2003/0018913, paragraph 44.
[9] See Brezak, U.S. Pat. Pub. No. 2003/0018913, paragraph 44.

authentication database 208, or the authentication service may simply copy relevant PAC data from the client's service ticket if that ticket included the first PAC[10]. The relevant transactions in Brezak are seen in the illustration presented below.



Thus, contrary to the Examiner's arguments[11], Brezak *cannot* teach or suggest "...providing the signed common nonce to the plurality of servers as a signature for transactions so as to authenticate the client to the plurality of servers". This can be seen because the client's service ticket (including the first PAC in the client service ticket, if present) never makes it to the back-end server, e.g., server C. Rather, the PAC in the client service ticket is used as a tool by Server A to request its *own* service ticket, which may include a second PAC, which is used to request yet another ticket in the delegation/transaction with the Server C[12] on behalf of the client 202.

Ganesan is Not Combinable With Brezak As Suggested By The Examiner

The Examiner acknowledges that Brezak does not disclose the client signing a common nonce. However, the Examiner argues that Ganesan teaches that in a ticketing system, to protect against dictionary attacks, the ticket should be encrypted by the ticket granting system with the key shared between the server to be accessed and the ticket granting server[13].

[10] See Brezak, U.S. Pat. Pub. No. 2003/0018913, paragraphs 45-49.
[11] See Office Action mailed 08/18/2006, Page 3, lines 23-25.
[12] See Brezak, U.S. Pat. Pub. No. 2003/0018913, paragraph 55.
[13] See Office Action mailed 08/18/2006, Page 4, lines 1-11.

Ganesan is directed to split private key asymmetric cryptography, where a message, including a ticket to access a server 50, is encrypted/signed and then verified to authenticate a client 10 to a server 50[14]. Accordingly, even Ganesan fails to teach or suggest "...providing the common nonce to the client" where the common nonce is "... associated with each of the plurality of servers from an entity other than the client or the plurality of servers" as claimed.

Regardless, if one were to try to employ the teachings of Ganesan as the Examiner suggests, the combination still fails to teach or suggest "...providing the signed common nonce to the plurality of servers as a signature for transactions so as to authenticate the client to the plurality of servers" as claimed because Server A merely forwards the client's service ticket (signed or not) with a first PAC to the authentication service 206[15] and receives a *new service ticket* with a *different* PAC from the authentication service 206, which is used to implement additional transactions, e.g., with Server C, as described above[16].

Conclusion

Accordingly, when considering claim 1 *as a whole*, the prior art references, whether taken singly or in combination, fail to teach or suggest all of the claimed limitations. As such, *no prima facie* case of obviousness has been established. Accordingly, the applicants respectfully request that claim 1 and the claims that depend there from, be withdrawn. Claims 26-28, 31, and 32 similarly recite such a common nonce, and are thus patentable for similar reasons. Also, dependent claims 2-22 and 30 are patentable at least per the patentability of Claims 1 and 28 from which they respectively depend.

Respectfully submitted,
Stevens & Showalter, L.L.P.
By

Thomas E. Lees 46,867

[14] See Ganesan, U.S. Pat. No. 5,532,276, Col. 5, lines 34-56 and Col. 15, lines 45-60.
[15] See Brezak, U.S. Pat. Pub. No. 2003/0018913, paragraph 45.
[16] See Brezak, U.S. Pat. Pub. No. 2003/0018913, paragraph 48.